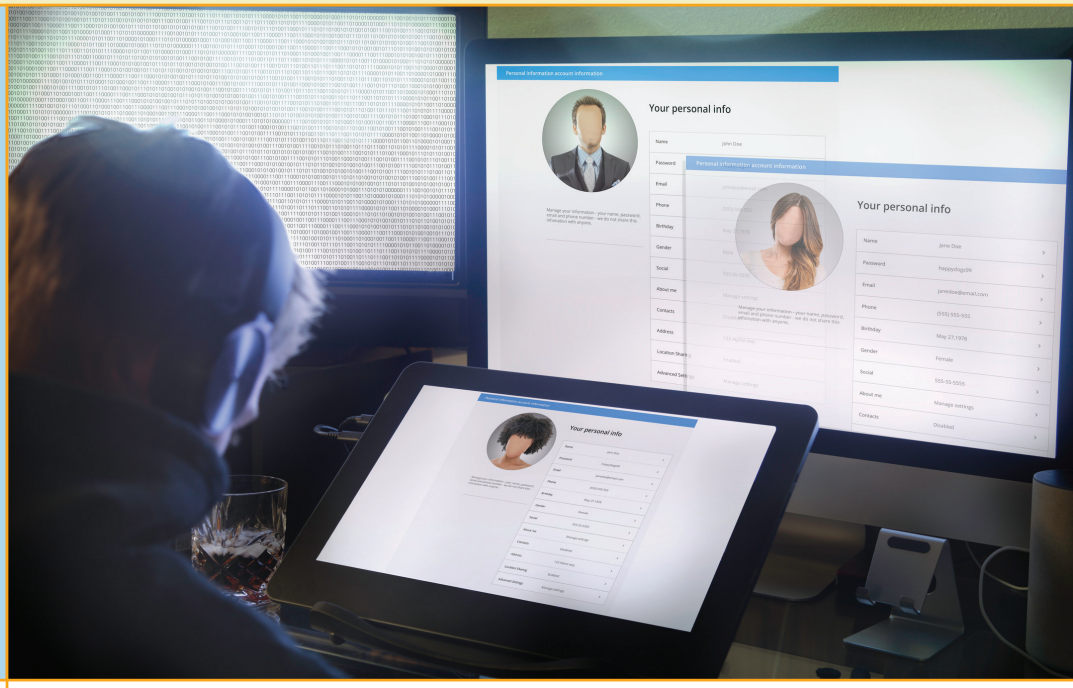
chapter 4

The Role of People in Security

We can prescribe actions, but not attitudes, and attitude is the secret sauce of security.

—W. A. Conklin



In this chapter, you will learn how to

- Define basic terminology associated with social engineering
- Describe steps organizations can take to improve their security
- Describe common user actions that may put an organization's information at risk
- Recognize methods attackers may use to gain information about an organization
- Determine ways in which users can aid instead of detract from security
- Recognize the roles training and awareness play in assisting the people side of security

The operational model of computer security discussed in the previous chapter acknowledges that absolute protection of computer systems and networks is not possible and that we need to be prepared to detect and respond to attacks that are able to circumvent our security mechanisms. Another very basic fact that should be recognized is that technology alone will not solve the security problem. No matter how advanced the technology is, it will ultimately be deployed in an environment where humans exist. It is the human element that poses the biggest security challenge. It is hard to compensate for all the possible ways humans can deliberately or accidentally cause security problems or circumvent our security mechanisms. Despite all the technology, despite all the security procedures we have in place, and despite all the security training we may provide, somebody will invariably fail to do what they are supposed to do, or do something they are *not* supposed to do, and create a vulnerability in the organization's security posture. This chapter discusses the human element and the role that people play in security—both the user practices that can aid in securing an organization and the vulnerabilities or holes in security that users can introduce.

People—A Security Problem

The operational model of computer security acknowledges that prevention technologies are not sufficient to protect our computer systems and networks. There are a number of explanations for why this is true; most of them are technical, but one of the biggest reasons that prevention technologies are not sufficient is that every network and computer system has at least one human user, and humans are prone to make mistakes and are often easily misled or fooled.

Social Engineering

Social engineering is the process of an unauthorized individual convincing an authorized individual to provide them with confidential information or access to something that they shouldn't have. It is a technique in which the attacker uses various deceptive practices to convince the targeted person to divulge information they normally would not divulge or to convince the target of the attack to do something they normally wouldn't do. Social engineering is very successful for several reasons. The first is the basic desire of most people to be helpful. When somebody asks a question for which we know the answer, our normal response is not to be suspicious but rather to answer the question. The problem with this is that seemingly innocuous information can be used either directly in an attack or indirectly to build a bigger picture that an attacker can use to create an aura of authenticity during an attack—the more information an individual has about an organization, the easier it will be to convince others that this person is part of the organization and has a right to even sensitive information. An attacker who is attempting to exploit the natural tendency of people to be helpful may take one of several approaches:

- The attacker might simply ask a question, hoping to immediately obtain the desired information. For basic information that is not considered sensitive, this approach generally works. As an example, an attacker might call and ask who the IT manager is.
- The attacker might first attempt to engage the target in conversation and try to evoke sympathy so that the target feels sorry for the individual and is more prone to provide the information. For information that is even slightly sensitive in nature, the request of which could possibly arouse suspicion, this technique may be tried. As an example, an attacker might call and claim to be under some deadline from a supervisor who is upset for some reason. The target, feeling sorry for an alleged fellow worker, might give up the information, thinking they are helping them avoid trouble with the supervisor.
- The attacker might appeal to an individual's ego. As an example, an attacker might call the IT department, claiming to have some sort of problem, and praising them for work they supposedly did to help another worker. After being told how great they are and how much they helped somebody else, the IT department might be tempted to demonstrate that they can supply the same level of help to another individual. This technique may be used to obtain sensitive information, such as having the target's password reset.

Tech Tip

Social Engineering Works!

Skilled social engineers set up scenarios where the victim is boxed in by various social/work issues and then makes an exception that enables the social engineer to gain some form of access. The attacker can pretend to be an important party and intimidate a lower-level employee, or he can create a sense of emergency, scarcity, or urgency that moves the victim to act in a manner to reduce the conflict. The attacker can become a "victim," creating a sense of fellowship with the target, creating a false sense of familiarity, and then using that to drive an action. Social engineers can sell ice to Eskimos and make them proud of their purchase, so they are masters at psychological manipulation.

The second reason that social engineering is successful is that individuals normally seek to avoid confrontation and trouble. If the attacker attempts to intimidate the target, threatening to call the target's supervisor because of a lack of help, the target may give in and provide the information to avoid confrontation. This variation on the attack is often successful in organizations that have a strict hierarchical structure. In the military, for example, a lower-ranking individual may be coerced into providing information to an individual claiming to be of higher rank or to be working for another individual higher up in the chain of command.

Social engineering can also be accomplished using other means besides direct contact between the target and the attacker. For example, an attacker might send a forged e-mail with a link to a bogus website that has been set up to obtain information from the target or convince the target to perform some action. Again, the goal in social engineering is to convince the target to provide information that they normally wouldn't divulge or to perform some act that they normally would not do. An example of a slightly different attack that is generally still considered social engineering is one in which an attacker replaces the blank deposit slips in a bank's lobby with ones containing his or her own account number but no name. When an unsuspecting customer uses one of the slips, a teller who is not observant could end up crediting the attacker's account with the deposit.

Tools

The tools in a social engineer's toolbox are based on a knowledge of psychology and don't necessarily require a sophisticated knowledge of software or hardware. The social engineer will employ strategies aimed at exploiting people's own biases and beliefs in a manner to momentarily deny them the service of good judgment and the use of standard procedures. Employing social engineering tools is second nature to a social engineer, and with skill they can switch these tools in and out in any particular circumstance, just as a plumber uses various hand tools and a system administrator uses OS commands to achieve complex tasks. When watching any of these professionals work, we may marvel at how they wield their tools, and the same is true for social engineers—except their tools are more subtle, and the target is people and trust. The following sections detail common "techniques" that can be employed in many social engineering attacks.

Principles (Reasons for Effectiveness)

Social engineering is very successful for two general reasons. The first is the basic desire of most people to be helpful. When somebody asks a question for which we know the answer, our normal response is not to be suspicious but rather to answer the question. The problem with this is that seemingly innocuous information can be used either directly in an attack or indirectly to build a bigger picture that an attacker can use to create an aura of authenticity during an attack—the more information an individual has about an organization, the easier it will be to convince others that she is part of the organization and has a right to even sensitive information.

The second reason that social engineering is successful is that individuals normally seek to avoid confrontation and trouble. If the attacker attempts to intimidate the target, threatening to call the target's supervisor because of a lack of help, the target may give in and provide the information to avoid confrontation.

The effectiveness of social engineering attacks is part technical and part psychological. For an attack to trick most users, psychological hooks are used to make the attacker more effective in getting a user to perform a desired action. Understanding the psychological component of these attacks is important.

Authority

The use of **authority** in social situations can lead to an environment where one party feels at risk in challenging another over an issue. If an attacker can convince a target that he has authority in a particular situation, he can entice the target to act in a particular manner or risk adverse consequences. In short, if you act like a boss when requesting something, people are less likely to withhold it.

The best defense against this and many social engineering attacks is a strong set of policies that has no exceptions. Much like security lines in the airport, when it comes to the point of screening, everyone gets screened, even flight crews, so there is no method of bypassing the critical step.

Intimidation

Intimidation can be either subtle, through perceived power, or more direct, through the use of communications that build an expectation of superiority.

Consensus

Consensus is a group-wide decision. It frequently comes not from a champion, but rather through rounds of group negotiation. These rounds can be manipulated to achieve desired outcomes. The social engineer simply motivates others to achieve her desired outcome.

Scarcity

If something is in short supply and is valued, then arriving with what is needed can bring rewards—and acceptance. "Only *X* widgets left at this price" is an example of this technique. Even if something is not scarce, implied scarcity, or implied future change in availability, can create a perception of scarcity. By giving the impression of **scarcity**, or short supply, of a desirable product, an attacker can motivate a target to make a decision quickly without deliberation.

Familiarity

People do things for people they like or feel connected to. Building this sense of **familiarity** and appeal can lead to misplaced trust. The social engineer can focus the conversation on familiar items, not the differences. Again, by leading with persuasion, a social engineer can convince someone that he has "been there before" or has done something, even if he hasn't, and this perception will lead to the desired familiar feeling on the part of the victim.

Trust

Trust is defined as having an understanding of how something will act under specific conditions. Social engineers can shape the perceptions of a target to where they will apply judgments to the trust equation and come to false conclusions. The whole objective of social engineering is not to force

The key in all social engineering attacks is that you are manipulating a person and their actions by manipulating their perception of a situation. A social engineer preys on people's beliefs, biases, and stereotypes—to the victim's detriment. This is hacking the human side of a system.

people to do things they would not do, but rather to give them a pathway that leads them to feel they are doing the correct thing in the moment.

Urgency

Time can be manipulated to drive a sense of **urgency** and prompt shortcuts that can lead to opportunities for interjection into processes. Limited-time offers should always be viewed as suspect. Perception is the key. Giving the target a reason to believe that they can take advantage of a time situation, whether it really is present or not, achieves the outcome of them acting in a desired manner.

Defenses

In all of the cases of impersonation, the best defense is simple—have processes in place that require employees to ask to see a person's ID before engaging with them if the employees do not personally know them. That includes challenging people such as delivery drivers and contract workers. Don't let people in through the door, tailgating/piggybacking, without checking their ID. If this is standard process, then no one becomes offended, and if someone fakes offense, it becomes even more suspicious. Training and awareness do work, as proven by trends such as the diminished effectiveness of pop-up windows. But the key to this defense is to make the training periodic and to tailor it to what is currently being experienced, rather than a generic recitation of best practices.

A training and awareness program is still the best defense against social engineering attacks.

Phishing, smishing, vishing—these are attacks against users' cognitive state. Using the principles (reasons for effectiveness) discussed earlier in the chapter, one can craft a message that makes falling victim to such an attack more likely. The attack is a combination of a technical element and psychological pressure, and together the user takes the bait and clicks the link.

Attacks

Social engineering attacks target the people portion of your computing environment. Using psychology and technical means, the social engineer attempts to get a user to perform specific actions on a system—actions they normally would not do. These include clicking a link and going to a web page, running a program, saving information, and opening a file. The list is long, and the means of defense is not against the technical but rather against the psychology side of the problem. Training users to think before they click is important.

Impersonation

Impersonation is a common social engineering technique that can be employed in many ways. It can occur in person, over a phone, or online. In the case of an impersonation attack, the attacker assumes a role that is recognized by the person being attacked, and in assuming that role, the attacker uses the potential victim's own biases against their better judgment to follow procedures. Impersonation can take a variety of forms—third parties, help desk operators, vendors, and even online sources.

Third-Party Authorization

Using previously obtained information about a project, deadline, boss, and so on, the attacker (1) arrives with something the victim is somewhat

expecting or would see as normal, (2) uses the guise of a project in trouble or some other situation where the attacker will be viewed as helpful or as someone not to upset, and (3) name-drops "Mr. Big," who happens to be out of the office and unreachable at the moment, thus avoiding a reference check. Note that the attacker seldom asks for anything that on the face of it seems unreasonable or is unlikely to be shared based on the circumstances. These actions can create the appearance of a third-party authorization, when in fact there is none.

Contractors/Outside Parties

It is common in many organizations to have outside contractors clean the building, water the plants, and perform other routine chores. In many of these situations, without proper safeguards, an attacker can simply put on clothing that matches a contractor's uniform, show up to do the job at a slightly different time than it's usually done, and, if challenged, play on the sympathy of the workers by saying they are filling in for *X* or covering for *Y*. The attacker can then roam the halls unnoticed because they blend in, all the while photographing desks and papers and looking for information.

Help Desk/Tech Support

Calls to or from help desk and tech support units can be used to elicit information. Posing as an employee, a social engineer can get a password reset, details about some system, and other useful information. The call can go the other direction as well, where the social engineer is posing as the help desk or tech support. Then, by calling employees, the attacker can get information on system status and other interesting elements that they can use later.

Online Attacks

Impersonation can be employed in online attacks as well. In these cases, technology plays an intermediary role in the communication chain. Some older forms, such as pop-up windows, tend to be less effective today because users are wary of them. Yet phishing attempts via e-mail and social media scams abound.

Up to this point, social engineering has been discussed in the context of an outsider attempting to gain information about the organization. This does not have to be the case. Insiders may also attempt to gain information they are not authorized to have. In many cases, the insider can be much more successful because they will already have a certain level of information regarding the organization and can therefore better spin a story that might be believable to other employees.

Phishing

Phishing (pronounced "fishing") is a type of social engineering in which an attacker attempts to obtain sensitive information from users by masquerading as a trusted entity in an e-mail or instant message sent to a large group of often random users. The attacker attempts to obtain information such as usernames, passwords, credit card numbers, and details about the users' bank accounts. The message that is sent often encourages the user to go to a website that appears to be for a reputable entity such as PayPal or eBay, both of which have frequently been used in phishing attempts. The website the user actually visits is not owned by the reputable organization, however, and asks the user to supply information that can be used in a later attack. Often the message sent to the user states that the user's account has been compromised and requests that they, for security purposes, enter their account information to verify the details.

Phishing is now the most common form of social engineering attack related to computer security. The target could be a computer system and access to the information found on it (such as is the case when the phishing attempt asks for a user ID and password), or it could be personal information, generally financial, about an individual (in the case of phishing attempts that ask for an individual's banking information).

In another very common example of phishing, the attacker sends a bulk e-mail, supposedly from a bank, telling the recipients that a security breach has occurred and instructing them to click a link to verify that their account has not been tampered with. If an individual actually clicks the link, they are taken to a site that appears to be owned by the bank but is actually controlled by the attacker. When they supply their account and password for "verification" purposes, they are actually giving it to the attacker.

Smishing

Smishing is a version of a phishing attack using Short Message Service (SMS) on victims' cell phones. It begins with an SMS message directing a user to a URL from which the attacker then can serve up a variety of attack vectors, including forms of malware. This attack works primarily because of the principles of urgency and intimidation, spurred by warnings such as "You are subscribed to XYZ service, which will begin regular billings of $2 a month. Click here to unsubscribe before billing takes place." Then, when the user clicks the URL, the next phase of the attack can begin.

Vishing

Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking. Vishing takes advantage of the trust that some people place in the telephone network. Users are unaware that attackers can spoof (simulate) calls from legitimate entities using Voice over IP (VoIP) technology. Voice messaging can also be compromised and used in these attempts. This is used to establish a form of trust that is then exploited by the attacker over the phone. Generally, the attackers are hoping to obtain credit card numbers or other information that can be used in identity theft. The user may receive an e-mail asking them to call a number that is answered by a potentially compromised voice message system. Users may also receive a recorded message that appears to come from a legitimate entity. In both cases, the user will be encouraged to respond quickly and provide the sensitive information so that access to their account is not blocked. If a user ever receives a message that claims to be from a reputable entity and asks for sensitive information, the user should not provide it but instead should use the Internet or examine a legitimate account statement to find a phone number that can be used to contact the entity. The user can then verify that the message received was legitimate or report the vishing attempt.

A great video showing the use of several social engineering tools can be found at https://www.youtube.com/watch?v=lc7scxvKQOo ("This is how hackers hack you using simple social engineering"). This video demonstrates the use of vishing to steal someone's cell phone credentials.

Tech Tip

Beware of Vishing

Vishing (phishing conducted using voice systems) is generally successful because of the trust that individuals place in the telephone system. With caller ID, people believe they can identify who is calling them. They do not understand that, just like many protocols in the TCP/IP protocol suite, caller ID can be spoofed.

Spam

Spam, as just about everybody knows, is bulk unsolicited e-mail. Though not generally considered by many as a social engineering issue, or even a security issue for that matter, spam can still be a security concern. It can be legitimate in the sense that it has been sent by a company advertising a product or service, but it can also be malicious and could include an attachment that contains malicious software designed to harm your system, or a

link to a malicious website that may attempt to obtain personal information from you. Because spam is unsolicited, you should always consider the source before clicking any links or directly responding. In this regard, the fact that spam can result in users clicking links, this is a form of social engineering due to altering human behavior.

Spam over Internet Messaging (SPIM)

Though not as well known, a variation on spam is **SPIM**, which is basically spam delivered via an instant messaging application. The purpose of hostile SPIM is the same as that of spam—the delivery of malicious content or links and getting an unsuspecting user to click them, thus initiating the attack.

Spear Phishing

Spear phishing is the term that has been created to refer to a phishing attack that targets a specific group of people or businesses with something in common. Because a specific group is being targeted, such as senior executives, the ratio of successful attacks (that is, the number of responses received) to the total number of e-mails or messages sent usually increases because a targeted attack will seem more plausible than a message sent to users randomly.

Whaling

High-value targets are referred to as whales. A **whaling** attack is thus one where the target is a high-value person, such as a CEO or CFO. Whaling attacks are not performed by attacking multiple targets and hoping for a reply, but rather are custom-built to increase the odds of success. Spear phishing is a common method used against whales, as it is designed to appear to be ordinary business for the target, being crafted to imitate a non-suspicious communication. Whales can be deceived in the same manner as any other person; the difference is that the target group is limited, hence an attacker cannot rely upon random returns from a wide population of targets.

Pharming

Pharming consists of misdirecting users to fake websites made to look official. Using phishing, attackers target individuals, one by one, by sending out e-mails. To become a victim, the recipient must take an action (for example, respond by providing personal information). In pharming, the user will be directed to the fake website as a result of activity such as DNS poisoning (an attack that changes URLs in a server's domain name table) or modification of local host files (which are used to convert URLs to the appropriate IP address). Once at the fake site, the user might supply personal information, believing that they are connected to the legitimate site.

Tech Tip

Defense Against Social Engineering Attacks

Defending against social engineering attacks, where the technical aspects are beyond your immediate control, as in pharming, seems daunting. Yet, there is a common element to these attacks: the user. Users need to be aware of how social engineers will attack and that they are the social engineers' target. Having users receive periodic training, on a regular basis in very small pieces, has been shown to be effective at improving awareness and detection. Little cues, misspellings, colors, and formats can provide clues that something isn't right. Being asked to do something that is different from the norm, logging in again, and asking for information or actions that are not normal—these are all signs of manipulation. When viewed as someone trying to manipulate you, this can be more noticeable.

Dumpster Diving

The process of going through a target's trash in hopes of finding valuable information that might be used in a penetration attempt is known in the security community as **dumpster diving**. One common place to find information, if the attacker is in the vicinity of the target, is in the target's trash. The attacker might find little bits of information that could be useful for an attack. The tactic is not, however, unique to the computer community; it has been used for many years by others, such as identity thieves, private investigators, and law enforcement personnel, to obtain information about an individual or organization. If the attackers are very lucky, and the target's security procedures are very poor, they may actually find user IDs and passwords.

An attacker may gather a variety of information that can be useful in a social engineering attack. In most locations, trash is no longer considered private property after it has been discarded (and even where dumpster diving is illegal, little enforcement occurs). An organization should have policies about discarding materials. Sensitive information should be shredded, and the organization should consider securing the trash receptacle so that individuals can't forage through it. People should also consider shredding personal or sensitive information that they wish to discard in their own trash. A reasonable quality shredder is inexpensive and well worth the price when compared with the potential loss that could occur as a result of identity theft.

Shoulder Surfing

Shoulder surfing does not necessarily involve direct contact with the target, but instead involves the attacker directly observing the individual entering sensitive information on a form, keypad, or keyboard. The attacker may simply look over the shoulder of the user at work, for example, or may set up a camera or use binoculars to view the user entering sensitive data. The attacker can attempt to obtain information such as a personal identification number (PIN) at an automated teller machine (ATM), an access control entry code at a secure gate or door, or a calling card or credit card number. Many locations now use a privacy screen or filter to surround a keypad so that it is difficult to observe somebody as they enter information. More sophisticated systems can actually scramble the location of the numbers so that the top row at one time includes the numbers 1, 2, and 3 and the next time includes 4, 8, and 0. While this makes it a bit slower for the user to enter information, it thwarts an attacker's attempt to observe what numbers are pressed and then enter the same buttons/pattern, since the location of the numbers constantly changes.

A related, somewhat obvious security precaution is that a person should not use the same PIN for all of their different accounts, gate codes, and so on, because an attacker who learns the PIN for one type of access could then use it for all the other types of access.

Although methods such as adding shields to block the view and having the pad scramble the numbers can help make shoulder surfing more difficult, the best defense is for users to be aware of their surroundings and to not allow individuals to get into a position from which they can observe what the user is entering.

The attacker may attempt to increase the chance of successfully observing the target entering the data by starting a conversation with the target.

This provides an excuse for the attacker to be physically closer to the target. Otherwise, the target could be suspicious if the attacker is standing too close. In this sense, shoulder surfing can be considered a social engineering attack.

Tailgating/Piggybacking

Tailgating (or **piggybacking**) is the simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building. People are often in a hurry and will frequently not follow good physical security practices and procedures. Attackers know this and may attempt to exploit this characteristic in human behavior. An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card. It is similar to shoulder surfing in that it relies on the attacker taking advantage of an authorized user who is not following security procedures. Frequently the attacker may even start a conversation with the target before reaching the door so that the user may be more comfortable with allowing the individual in without challenging them. In this sense, piggybacking is related to social engineering attacks.

Both the piggybacking and shoulder surfing attack techniques rely on the poor security practices of an authorized user in order to be successful. Thus, both techniques can be easily countered by training employees to use simple procedures to ensure nobody follows them too closely or is in a position to observe their actions. A more sophisticated countermeasure to piggybacking is a *mantrap*, which utilizes two doors to gain access to the facility. The second door does not open until the first one is closed, and the doors are closely spaced so that an enclosure is formed that only allows one individual through at a time.

Cross Check

Mantraps, tailgating, and other personal security items related to physical access are covered in Chapter 8. You will find a great picture of a mantrap there as well.

Eliciting Information

Calls to or from help desk and tech support units can be used to *elicit information*. A skilled social engineer can use a wide range of psychological techniques to convince people, whose main job is to help others, to perform tasks resulting in security compromises. Posing as an employee, an attacker can get a password reset, information about some system, or other useful information. The call can go the other direction as well, where the social engineer is posing as the help desk or tech support. Then, by calling employees, the attacker can get information on system status and other interesting elements that they can use later.

Prepending

Prepending is defined as the act of adding something else to the beginning of an item. When used in a social engineering context, prepending is the act of supplying information that another will act upon, frequently before they ask for it, in an attempt to legitimize the actual request, which comes later. Using the psychological constructs of authority, prepending can take the form of the attacker stating that they are sent by someone's boss, or another authority figure, as a means to justify why the victim of the attack should perform a specific action—typically one that, in the absence of the prepend, would not be normal.

Identity Fraud

Identity fraud is the use of fake credentials to achieve an end. This can be a high-risk endeavor, such as pretending to be an official representative of a government agency or a regulator, or it can be lower risk, such as showing up as the person who waters the plants. One could pretend to be a delivery agent, show up with a box—or better yet, a server—and attempt direct delivery to the server room. This works best when the victim is expecting the person, as in the case of a broken server under a repair warranty. Identity fraud can be done online as well, using known information about the person being impersonated (see the "Impersonation" section earlier in the chapter) and deceiving the victim being attacked. Defense against identity fraud is the same as most other social engineering attacks—use strong policies and procedures, without exceptions (for example, all packages must be dropped at the security desk, all visitors who need access must be escorted 100 percent of the time, and so on). Also, there should be no exceptions on disclosure policies, such as resetting passwords and giving a third party access. Doing everything by the rules works. Just look at TSA security—there is no way past their line without being screened first. The accuracy and effectiveness of their screening may be legitimately questioned, but getting around it is not. This is key for stopping most social engineering attacks.

Invoice Scams

Invoice scams are just that—a scam using a fake invoice in an attempt to get a company to pay for things it has not ordered. The premise is simple: send a fake invoice and then get paid. In practice, since most companies have fairly strong accounting controls, the scam involves getting someone outside of the accounting group to initiate the process, thus lending a sense of legitimacy. This all seems like it wouldn't work, yet cybercriminals collect billions of dollars per year using this method. Common items used in these scams are office products such as toner and normal office supplies, cleaning products, organizational memberships, and a wide range of corporate services. Sometimes, to add urgency, the attacker includes a final notice, threatening to involve a collection agency, making a person hesitate before just throwing the bill away.

Credential Harvesting

Credential harvesting is the collection of credential information, such as user IDs, passwords, and so on, thus allowing an attacker a series of passes to the system. A common form of credential harvesting starts with a phishing e-mail that convinces a user to click a link and, in response, brings up a replica of their bank's web page. It looks like the bank's page (and users typically do not check the security settings of their browser connection), and when the user enters their credentials, the credentials (user ID and password) are harvested and stored for later use by the criminal.

The objective of a credential harvest is just that—credentials. Once the criminal has tricked you into providing your credentials, they will either redirect you to the correct website or provide an error and a new connection to the correct website for you to try again. The objective is to make you think everything is working and to mask the fact that they stole your credentials. This attack method has been highly successful, and it is now standard practice for financial firms to follow normal user ID and password with a second factor, such as an out-of-band inquiry, to prevent subsequent use of harvested credentials. While this adds a layer of complexity and inconvenience to the user, it has become an accepted practice and is necessary to prevent harvested credential reuse.

Many of the attacks are designed to get a user's credentials. Any credentials you can share comprise a risk, and to combat this risk, organizations have adopted two-factor authentication. The second factor is a different method of identifying the user and is typically unique and only valid for a limited time. An example is when you log in to your bank, and you get a text message with a code to authorize entry. This code significantly complicates the problem for an attacker if they get your credentials.

Reverse Social Engineering

A slightly different approach to social engineering is called **reverse social engineering**. In this technique, the attacker hopes to convince the target to initiate the contact. This obviously differs from the traditional approach, where the target is the one who is contacted. The reason this attack might be successful is that, because the target is the one initiating the contact, attackers might not have to convince the target of their authenticity. The tricky part of this attack is, of course, convincing the target to make that initial contact. One possible method for accomplishing this involves sending out a spoofed e-mail (a fake e-mail designed to appear authentic) that claims to be from a reputable source and provides another e-mail address or phone number to call for "tech support." Another method might be posting a notice or creating a bogus website for a legitimate company that also claims to provide "tech support." This may be especially successful if timed to coincide with a company's deployment of a new software or hardware platform. Another potential time to target an organization with this sort of attack is when there is a significant change in the organization itself, such as when two companies merge or a smaller company is acquired by a larger one. During these times, employees are not familiar with the new organization or its procedures, and amid the confusion it is easy to conduct either a social engineering or reverse social engineering attack.

Tech Tip

Be Aware of Reverse Social Engineering

Reverse social engineering is not nearly as widely understood as social engineering and is a bit trickier to execute. If the attacker is successful in convincing an individual to make the initial contact, however, the process of convincing that individual of their authenticity is generally much easier than in a social engineering attack.

Reconnaissance

Reconnaissance is a military term used to describe the actions of surveying a battlefield to gain information prior to hostilities. In the field of cybersecurity, the concept is the same—an adversary will examine the systems they intend to attack, using a wide range of methods. Some of these methods do

not involve directly engaging the victim—Google searches, public record searches, and so on. But other aspects are involved in directly manipulating people to gain information. Obtaining and then surveying org charts, calling and asking for contact information on people and then building a personnel directory, asking questions about hardware and software via surveys—all of these methods provide information that goes into a description of the system that will be under attack. While most reconnaissance is accepted as inevitable, some of it is helped via items such as press releases telling the world who your security partners are, what products you are employing, and so on. Each of these items of information will be used later as part of the attack process. Known weaknesses against specific products can be employed and are easier to find if the attacker knows what products a company is using. Performing a solid reconnaissance before attacking provides the attacker with key informational elements later when the items are needed.

Hoax

At first glance, it might seem that a **hoax** related to security would be considered a nuisance and not a real security issue. This might be the case for some hoaxes, especially those of the urban legend type, but the reality of the situation is that a *hoax* can be very damaging if it causes users to take some sort of action that weakens security. One real hoax, for example, described a new, highly destructive piece of malicious software. It instructed users to check for the existence of a certain file and to delete it if the file was found. In reality, the file mentioned was an important file used by the operating system, and deleting it caused problems the next time the system was booted. The damage caused by users modifying security settings can be serious. As with other forms of social engineering, training and awareness are the best and first line of defense for both users and administrators. Users should be trained to be suspicious of unusual e-mails and stories, and they should know who to contact in the organization to verify the validity these e-mails if they are received. A hoax e-mail often also advises the user to send it to their friends so that they know about the issue as well—and by doing so, they help spread the hoax. Users need to be suspicious of any e-mail telling them to "spread the word."

Watering Hole Attack

The most commonly recognized attack vectors are those that are direct to a target. Because of their incoming and direct nature, the attack vectors require defenses to be crafted to detect and defend against them. But what if the user "asks" for the attack by visiting a website? Just as a hunter waits near a watering hole for animals to come drink, attackers can plant malware at sites where users are likely to frequent. First identified by RSA, a security firm, a *watering hole attack* involves the infecting of a target website with malware. In some of the cases detected, the infection was constrained to a specific geographical area. These are not simple attacks, yet they can be very effective at delivering malware to a specific groups of end users. Watering hole attacks are complex to achieve and appear to be backed by

nation-states and other high-resource attackers. In light of the stakes, the typical attack vector will be a zero-day attack to further avoid detection.

Different threat actors, such as nation-states, and attack vectors are discussed in Chapter 15.

Typo Squatting

Typo squatting is an attack form that involves capitalizing on common typographical errors. If a user mistypes a URL, then the result should be a 404 error, or "resource not found." But if an attacker has registered the mistyped URL, then the user would land on the attacker's page. This attack pattern is also referred to as *URL hijacking*, *using a fake URL*, or *brandjacking* if the objective is to deceive based on branding.

There are several reasons that an attacker will pursue this avenue of attack. The most obvious is one for a phishing attack. The fake site collects credentials, passing them on to the real site, and then steps out of the conversation to avoid detection once the credentials are obtained. It can also be used to plant drive-by malware on the victim machine. It can also move the packets through an affiliate network, earning click-through revenue based on the typos. There are numerous other forms of attacks that can be perpetrated using a fake URL as a starting point.

Influence Campaigns

Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people's minds on a topic. One can engage in an influence campaign against a single person, but the effect is limited. Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation. Influencers are people who have large followings of people who read what they post and, in many cases, act in accordance or agreement. This serves as an amplifying mechanism, where single pieces of disinformation can be rapidly spread to build a following across the Internet. The effects are strong enough that nation-states have used these techniques as a form of conflict, termed **hybrid warfare**, where the information is used to sway people toward a position favored by those spreading it. What makes this effective is the psychological effect of groups—in particular, the bandwagon effect, where when one person leads, and many follow, typically without critically examining the premise they are following. In previous wars, this was called propaganda. Today, with rapid communication worldwide via social media platforms, these methods are even more effective at moving mass belief in groups of populations.

Poor Security Practices

A significant portion of human-created security problems results from poor security practices. These poor practices may be from an individual user not following established security policies or processes, or they may be caused by a lack of security policies, procedures, or training within the user's organization.

Poor password selection is one of the most common of poor security practices, and one of the most dangerous. Numerous studies conducted on password selection have found that, while overall more users are learning to select good passwords, a significant percentage of users still make poor choices. The problem with this, of course, is that a poor password choice can enable an attacker to compromise a computer system or network more easily. Even when users have good passwords, they often resort to another poor security practice—writing their passwords down in an easily located place, which can also lead to system compromise if an attacker gains physical access to the area.

Writing down and hiding passwords doesn't work if someone has physical access. The number of hiding places that are convenient is few, and most security people know them all. Don't write them down—anywhere.

Password Selection

For many years, computer intruders have relied on users' poor selection of passwords to help them in their attempts to gain unauthorized access to systems and networks. If attackers could obtain a list of the users' names, chances were good they could eventually access the system. Users tend to pick passwords that are easy for them to remember, and what easier password could there be than the same sequence of characters that they use for their user ID? If a system has an account with the username *jdoe*, an attacker's reasonable first guess of the account's password would be *jdoe.* If this doesn't work, the attacker would try variations on the same, such as *doej, johndoe, johnd,* and *eodj,* all of which would be reasonable possibilities.

Organizations have also instituted additional policies and rules relating to password selection to further complicate an attacker's efforts. Organizations, for example, may require users to frequently change their password. This means that if an attacker is able to guess a password, it is only valid for a limited period of time before a new password is selected, after which the attacker is locked out. All is not lost for the attacker, however, because, again, users will select passwords they can remember. For example, password changes often result in a new password that simply incorporates a number at the end of the old one. Thus, a user might select *S3Cr3Tp4$$w0rD12* as a new password, replacing the version that ended in 11. This does not really add security because, if an attacker knew the old one, they can guess the next one.

The complexity of managing passwords has led to the creation of password manager programs. These programs, including the Chrome browser, attempt to make password management easier for users. There are good and bad aspects to these methods. First, if there is any way that a user can recover the password from the system, one must suspect the security. Chrome requires a user's password to return a stored password, but there are utilities that can scrape passwords from the system and display them. This means attackers can as well. Most password managers use encryption to secure their password stores, and this is good. However, once you become beholden to the system, if you lose your master password, you lose everything.

Tech Tip

Harvesting Passwords

In 2014, a vulnerability in the OpenSSL cryptography software library was discovered and given the name Heartbleed because it originated in the heartbeat signal employed by the system. This vulnerability resulted in the potential loss of passwords and other sensitive data across multiple platforms and up to a million web servers and related systems. Heartbleed resulted in random data loss from servers, as 64KB blocks of memory were exfiltrated from the system. Among the items that could be lost in Heartbleed attacks are user credentials, user IDs, and passwords. The discovery of this vulnerability prompted users to change a massive number of passwords across the Web, as users had no knowledge as to the status of their credentials. One of the common pieces of advice to users was to not reuse passwords between systems. This advice is universally good advice, not just for Heartbleed, but for all systems, all the time.

With the proliferation of computers, networks, and users, the password dilemma has gotten worse. Today, the average Internet user probably has at least a half dozen different accounts and passwords to remember. Selecting a different password for each account, following the guidelines mentioned previously regarding character selection and frequency of changes, only aggravates the problem of remembering the passwords. This results in users all too frequently using the same password for all accounts. If a user does this, and then one of the accounts is compromised, all other accounts are subsequently also vulnerable to attack.

The need for good password selection and the protection of passwords also applies to another common feature of today's electronic world: PINs. Most people have at least one PIN associated with their ATM card or a security code to gain physical access to a room. Again, users will invariably select numbers that are easy to remember. Specific numbers, such as the individual's birth date, their spouse's birth date, or the date of some other significant event, are all common numbers to select. Other people will pick patterns that are easy to remember—2580, for example, uses all of the center numbers on a standard numeric pad on a telephone. Attackers know this, and guessing PINs follows the same sort of process that guessing a password does.

Password selection is an individual activity, and ensuring that individuals are making good selections is the realm of the entity's password policy. In order for users make appropriate choices, they need to be aware of the issue and their personal role in securing accounts. An effective password policy conveys both the user's role and responsibility associated with password usage and does so in a simple enough manner that it can be conveyed via screen notes during mandated password change events.

Know the rules for good password selection. Generally, these are to use eight or more characters in your password, include a combination of upper- and lowercase letters, include at least one number and one special character, do not use a common word, phrase, or name, and choose a password you can remember so that you do not need to write it down. Also, don't reuse passwords.

Tech Tip

Passwordless Systems

Microsoft has provided users the option to go passwordless in Windows 10, but how is this secure? You can use a picture, a fingerprint, your face, or a simple PIN to unlock your Windows 10 machine. At first this system seems insecure, but it really isn't passwordless. There are still passwords behind the scenes. Microsoft is simply using a local proxy for the password to allow access to the machine. Any transactions across the network are still done with the same level of security. Your PIN, face, or biometric doesn't leave the machine; it just unlocks your password.

Shoulder Surfing

As discussed earlier, *shoulder surfing* does not involve direct contact with the user, but instead involves the attacker directly observing the target entering sensitive information on a form, keypad, or keyboard. The attacker may simply look over the shoulder of the user at work, watching as a coworker enters their password. Although defensive methods can help make shoulder surfing more difficult, the best defense is for a user to be aware of their surroundings and to not allow individuals to get into a position from which they can observe what the user is entering. A related security comment can be made at this point: a person should not use the same PIN for all of their different accounts, gate codes, and so on, because an attacker who learns the PIN for one could then use it for all the others.

Piggybacking

People are often in a hurry and will frequently not follow good physical security practices and procedures. Attackers know this and may attempt to exploit this characteristic in human behavior. *Piggybacking*, or tailgating, happens because the person is not paying attention to the context of their situation: they are passing a security checkpoint, so security should be their main focus. Frequently the attacker might even start a conversation with the target before reaching the door so that the user is more comfortable with

allowing the individual in without challenging them. In this sense, piggybacking is related to social engineering attacks. Both the piggybacking and shoulder surfing attack techniques can be easily countered by using simple procedures to ensure nobody follows you too closely or is in a position to observe your actions. Both techniques rely on the poor security practices of an authorized user to be successful.

Dumpster Diving

There may be a number of individuals who have access to a facility but are not authorized to access the information the systems store and process. We become complacent with the access these individuals have because they often quietly go about their job so as to not draw attention to themselves and to minimize the impact on the operation of the organization. They may also be overlooked because their job does not impact the core function of the organization. A prime example of this is the custodial staff. Becoming complacent about these individuals and not paying attention to what they may have access to, however, could be a big mistake, and users should not believe that everybody who has physical access to the organization has the same level of concern for or interest in the welfare of the organization.

As mentioned earlier, attackers need a certain amount of information before launching their attack. One common place to find this information, if the attacker is in the vicinity of the target, is the target's trash. The attacker might find little bits of information that could be useful for an attack. This process of going through a target's trash in hopes of finding valuable information that can be used in a penetration attempt is known in the computer community as *dumpster diving*.

This works because people are lazy and just throw things into the trash without thinking of the risk. Government offices with classified or important paperwork have specially marked "burn bags" where users can place items to be burned. Discipline is the key to avoiding laziness.

Try This!

Diving into Your Dumpster

The amount of useful information that users throw away in unsecured trash receptacles often amazes security professionals. Hackers know that they can often find manuals, network diagrams, and even user IDs and passwords by rummaging through dumpsters. After coordinating this with your security office, try seeing what you can find that individuals in your organization have discarded (assuming that there is no shredding policy) by either going through your organization's dumpsters or just through the office trash receptacles. What useful information did you find? Is there an obvious suggestion that you might make to enhance the security of your organization?

Installing Unauthorized Hardware and Software

Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems. A common example is a user installing unauthorized communication software and a modem to allow them to connect to their machine at work via a modem from their home. Another common example is a user installing a wireless access point so that they can access the organization's network from many different areas. In these examples, the user has set up a backdoor into the network, circumventing all the other security mechanisms in place. The terms *rogue modem* and *rogue access point* may be used to describe these two cases, respectively. A **backdoor** is an avenue that can be used to access a system while circumventing normal security mechanisms and can often be used to

install additional executable files that can lead to more ways to access the compromised system. Security professionals can use widely available tools to scan their own systems periodically for either of these rogue devices to ensure that users haven't created a backdoor.

Another common example of unauthorized software that users install on their systems is games. Unfortunately, not all games come in shrink-wrapped packages. Numerous small games can be downloaded from the Internet. The problem with this is that users don't always know where the software originally came from and what may be hidden inside it. Many individuals have unwittingly installed what seemed to be an innocuous game, only to have downloaded a piece of malicious code capable of many things, including opening a backdoor that allows attackers to connect to, and control, the system from across the Internet.

Because of these potential hazards, many organizations do not allow their users to load software or install new hardware without the knowledge and assistance of administrators. Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments that are sent to users. This helps prevent users from, say, unwittingly executing a hostile program that was sent as part of a worm or virus. Consequently, many organizations have their mail servers strip off executable attachments to e-mail so that users can't accidentally cause a security problem.

Data Handling

Understanding the responsibilities of proper data handling associated with one's job is an important training topic. Information can be deceptive in that it is not directly tangible, and people tend to develop bad habits around other job measures … at the expense of security. Employees require training in how to recognize the data classification and handling requirements of the data they are using, and they need to learn how to follow the proper handling processes. If certain data elements require special handling because of contracts, laws, or regulations, there is typically a training clause associated with this requirement. Personnel assigned to these tasks should be specifically trained with regard to the security requirements. The spirit of the training clause is you get what you train, and if security over specific data types is a requirement, then it should be trained. This same principle holds for corporate data-handling responsibilities: you get the behaviors you train and reward.

Preventing access to information is also important in the work area. Firms with sensitive information should have a "clean desk policy" specifying that sensitive information is not left unsecured in the work area when the worker is not present to protect the material.

Physical Access by Non-Employees

As has been mentioned, if an attacker can gain physical access to a facility, chances are very good that the attacker can obtain enough information to penetrate computer systems and networks. Many organizations require employees to wear identification badges when at work. This is an easy method to quickly spot who has permission to have physical access to the organization and who does not. Although this method is easy to implement and can be a significant deterrent to unauthorized individuals, it also requires that employees actively challenge individuals who are not wearing the required identification badge. This is one area where organizations fail. Combine an attacker who slips in by tailgating off of an authorized

If you work in a place where badges are required for access and you see someone without a badge, you should speak up. Hackers count on you not challenging them and not wanting to become involved. You don't have to make it personal; there is a policy, and policies don't push back. Just politely inquire as to whether they have lost their badge and, if so, escort them to the security desk for a new one.

individual and an environment where employees have not been encouraged to challenge individuals without appropriate credentials and you have a situation where you might as well not have any badges in the first place. Organizations also frequently become complacent when faced with what appears to be a legitimate reason to access the facility, such as when an individual shows up with a warm pizza claiming it was ordered by an employee. It has often been stated by security consultants that it is amazing what you can obtain access to with a pizza box or a vase of flowers.

Another aspect that must be considered is personnel who have legitimate access to a facility but also have the intent to steal intellectual property or otherwise exploit the organization. Physical access provides an easy opportunity for individuals to look for the occasional piece of critical information carelessly left out in the open. With the proliferation of devices such as cell phones with built-in cameras, an individual could easily photograph information without it being obvious to employees. Contractors, consultants, and partners frequently not only have physical access to the facility but may also have network access. Other individuals who typically have unrestricted access to the facility when no one is around are nighttime custodial crewmembers and security guards. Such positions are often contracted out. As a result, hackers have been known to take temporary custodial jobs simply to gain access to facilities.

Clean Desk Policies

Preventing access to information is also important in the work area. Firms with sensitive information should have a "clean desk policy" specifying that sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian. Even leaving the desk area and going to the bathroom can leave information exposed and subject to compromise. The clean desk policy should identify and prohibit certain actions that might not be obvious upon first glance, such as leaving passwords on sticky notes under keyboards or mouse pads or in unsecured desk drawers.

Per the multiple versions of the Verizon Data Breach Investigation Report, introduced in Chapter 1, hacks were discovered more often by internal employees than by outsiders. This means that trained users can be an important part of a security plan.

People as a Security Tool

An interesting paradox when speaking of social engineering attacks is that people are not only the biggest problem and security risk but also the best tool in defending against a social engineering attack. The first step a company should take to fight potential social engineering attacks is to create the policies and procedures that establish the roles and responsibilities for not only security administrators but for all users. What is it that management expects, security-wise, from all employees? What is it that the organization is trying to protect, and what mechanisms are important for that protection?

Security Awareness

Probably the single most effective method to counter potential social engineering attacks, after establishment of the organization's security goals and policies, is an active security awareness program. The extent of the training

will vary depending on the organization's environment and the level of threat, but initial employee training on social engineering at the time a person is hired is important, as well as periodic refresher training.

An important element that should be stressed in training about social engineering is the type of information that the organization considers sensitive and may be the target of a social engineering attack. There are undoubtedly signs that the organization could point to as indicative of an attacker attempting to gain access to sensitive corporate information. All employees should be aware of these indicators. The scope of information that an attacker may ask for is very large, and many questions attackers pose might also be legitimate in another context (asking for someone's phone number, for example). Employees should be taught to be cautious about revealing personal information and should especially be alert for questions regarding account information, personally identifiable information, and passwords.

Try This!

Security Awareness Programs

A strong security education and awareness training program can go a long way toward reducing the chance that a social engineering attack will be successful. Awareness programs and campaigns, which might include seminars, videos, posters, newsletters, and similar materials, are also fairly easy to implement and not very costly. There is no reason for an organization to not have an awareness program in place. A lot of information and ideas are available on the Internet. See what you can find that might be usable for your organization that you can obtain at no charge from various organizations on the Internet. (Tip: Check organizations such as NIST and the NSA that have developed numerous security documents and guidelines.)

As a final note on user responsibilities, corporate security officers must cultivate an environment of trust in their office, as well as an understanding of the importance of security. If users feel that security personnel are only there to make their life difficult or to dredge up information that will result in an employee's termination, the atmosphere will quickly turn adversarial and be transformed into an "us-versus-them" situation. Security personnel need the help of all users and should strive to cultivate a team environment in which users, when faced with a questionable situation, will not hesitate to call the security office. In situations like this, security offices should remember the old adage of "don't shoot the messenger."

Social Networking and P2P

With the rise in popularity of social networking sites—notably Facebook, Twitter, and LinkedIn—many people have gotten into a habit of sharing too much information. Using a status of "Returning from sales call to XYZ company" reveals information to people who have no need to know it. Confusing sharing information with friends and sharing business information with those who don't need to know it is a line people are crossing on a regular basis. Don't be the employee who mixes business and personal

information and releases information to parties who should not have it, regardless of how innocuous it may seem.

Users also need to understand the importance of not using common programs such as torrents and other peer-to-peer (P2P) file-sharing communication programs in the workplace, as these programs can result in infection mechanisms and data-loss channels. The information security training and awareness program should cover these issues. If the issues are properly explained to employees, their motivation to comply won't simply be to avoid adverse personnel action for violating a policy; they will want to assist in the security of the organization and its mission.

Security Policy Training and Procedures

People in an organization play a significant role in its security posture. As such, training is important because it can provide the basis for awareness of issues such as social engineering and desired employee security habits. These are detailed in Chapter 2.

Chapter 4 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following regarding the role people can play in security.

Define basic terminology associated with social engineering

- Social engineering is a technique in which the attacker uses various deceptive practices to convince the targeted person to divulge information they normally would not divulge, or to convince the target to do something they normally wouldn't do.
- In reverse social engineering, the attacker hopes to convince the target to initiate contact.

Describe steps organizations can take to improve their security

- Organizations should have a policy that restricts the ability of normal users to install new software and hardware on their systems.
- Contractors, consultants, and partners may frequently have not only physical access to the facility but also network access. Other groups that are given unrestricted, and unobserved, access to a facility are nighttime custodial crewmembers and security guards. Both are potential security problems, and organizations should take steps to limit these individuals' access.
- The single most effective method to counter potential social engineering attacks, after establishing the organization's security goals and policies, is an active security awareness program.

Describe common user actions that may put an organization's information at risk

- No matter how advanced security technology is, it will ultimately be deployed in an environment where the human element may be its greatest weakness.
- Attackers know that employees are frequently very busy and don't stop to think about security. They may attempt to exploit this work characteristic through piggybacking or shoulder surfing.

Recognize methods attackers may use to gain information about an organization

- For many years, computer intruders have relied on users' poor selection of passwords to help them in their attempts to gain unauthorized access to a system or network.
- One common way to find useful information (if the attacker is in the vicinity of the target, such as a company office) is to go through the target's trash looking for bits of information that could be useful to a penetration attempt.

Determine ways in which users can aid instead of detract from security

- An interesting paradox of social engineering attacks is that people are not only the biggest problem and security risk but also the best line of defense.
- A significant portion of employee-created security problems arises from poor security practices.
- Users should always be on the watch for attempts by individuals to gain information about the organization and should report suspicious activity to their employer.

Recognize the roles training and awareness play in assisting the people side of security

- Individual users can enhance security of a system through proper execution of their individual actions and responsibilities.
- Training and awareness programs can reinforce user knowledge of desired actions.

Key Terms

authority *(89)*
backdoor *(102)*
consensus *(89)*
credential harvesting *(97)*
dumpster diving *(94)*
familiarity *(89)*
hoax *(98)*
hybrid warfare *(99)*
identity fraud *(96)*
impersonation *(90)*
intimidation *(89)*
invoice scams *(96)*
pharming *(93)*
phishing *(91)*
piggybacking *(95)*
prepending *(96)*
reconnaissance *(97)*
reverse social engineering *(97)*
scarcity *(89)*
shoulder surfing *(94)*
social engineering *(87)*
smishing *(92)*
spam *(92)*
spam over Internet messaging (SPIM) *(93)*
spear phishing *(93)*
tailgating *(95)*
trust *(89)*
urgency *(90)*
vishing *(92)*
whaling *(93)*

Key Terms Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. A(n) _____ is an avenue that can be used to access a system while circumventing normal security mechanisms.
2. _____ is a procedure in which attackers position themselves in such a way as to be able to observe an authorized user entering the correct access code.
3. The process of going through a target's trash searching for information that can be used in an attack, or to gain knowledge about a system or network, is known as _____.
4. _____ is the simple tactic of following closely behind a person who has just used their access card or PIN to gain physical access to a room or building.
5. In _____, the attacker hopes to convince the target to initiate contact.
6. _____ is a variation of _____ that uses voice communication technology to obtain the information the attacker is seeking.
7. Social engineers will use psychological tools to mislead users into trusting them. Examples of these techniques include _____, _____, and _____.

Multiple-Choice Quiz

1. Which of the following is considered a good practice for password security?
   - **A.** Using a combination of upper- and lowercase characters, a number, and a special character in the password itself.
   - **B.** Not writing the password down.
   - **C.** Changing the password on a regular basis.
   - **D.** All of the above.
2. The password dilemma refers to which fact?
   - **A.** Passwords that are easy for users to remember are also easy for attackers to guess.
   - **B.** The more difficult we make it for attackers to guess our passwords, and the more frequently we force password changes, the more difficult the passwords are for authorized users to remember and the more likely they are to write them down.
   - **C.** Users will invariably attempt to select passwords that are words they can remember. This means they may select things closely associated with them, such as their spouse's or child's name, a beloved sports team, or a favorite model of car.
   - **D.** Passwords assigned by administrators are usually better and more secure, but are often harder for users to remember.
3. The simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building is called what?
   - **A.** Shoulder surfing
   - **B.** Tagging-along
   - **C.** Piggybacking
   - **D.** Access drafting
4. The process of going through a target's trash in hopes of finding valuable information that might be used in a penetration attempt is known as what?
   - **A.** Dumpster diving
   - **B.** Trash trolling
   - **C.** Garbage gathering
   - **D.** Refuse rolling
5. Which of the following is a type of social engineering attack in which an attacker attempts to obtain sensitive information from a user by masquerading as a trusted entity in an e-mail?
   - **A.** Spam
   - **B.** SPIM
   - **C.** Phishing
   - **D.** Vishing
6. Reverse social engineering involves which of the following?
   - **A.** Contacting the target, eliciting some sensitive information, and convincing them that nothing out of the ordinary has occurred
   - **B.** Contacting the target in an attempt to obtain information that can be used in a second attempt with a different individual
   - **C.** An individual lower in the chain of command convincing somebody at a higher level to divulge information that the attacker is not authorized to have
   - **D.** An attacker attempting to somehow convince the target to initiate contact in order to avoid questions about authenticity

7. Which of the following is a reason for not allowing users to install new hardware or software without the knowledge of security administrators?
   - **A.** They might not complete the installation correctly, and the administrator will have to do more work, taking them away from more important security tasks.
   - **B.** They might inadvertently install more than just the hardware or software; they could accidentally install a backdoor into the network.
   - **C.** They may not have paid for it and thus could be exposing the organization to civil penalties.
   - **D.** Unauthorized hardware and software are usually for leisure purposes and will distract employees from the job they were hired to perform.
8. Once an organization's security policies have been established, what is the single most effective method of countering potential social engineering attacks?
   - **A.** An active security awareness program
   - **B.** A separate physical access control mechanism for each department in the organization
   - **C.** Frequent testing of both the organization's physical security procedures and employee telephone practices
   - **D.** Implementing access control cards and wearing security identification badges
9. Which of the following types of attacks utilizes instant messaging services?
   - **A.** Spam
   - **B.** SPIM
   - **C.** Phishing
   - **D.** Vishing
10. Which of the following are psychological tools used by social engineers to create false trust with users?
   - **A.** Impersonation
   - **B.** Familiarity
   - **C.** Creating a sense of scarcity or urgency
   - **D.** All of the above

Essay Quiz

1. Explain the difference between social engineering and reverse social engineering.
2. Discuss how a security-related hoax might become a security issue.
3. How might shoulder surfing be a threat in your school or work environment? What can be done to make this sort of activity more difficult?
4. For an environment familiar to you (such as work or school), describe the different non-employees who might have access to facilities that could contain sensitive information.
5. Describe some of the user security responsibilities you feel are most important for users to remember.

Lab Projects

• Lab Project 4.1

If possible, at either your place of employment or your school, attempt to determine how easy it would be to perform dumpster diving to gain access to information at the site. Are trash receptacles easy to gain access to? Are documents shredded before being discarded? Are areas where trash is stored easily accessible?

• Lab Project 4.2

Perform a search on the Web for articles and stories about social engineering attacks or reverse social engineering attacks. Choose and read five or six articles. How many of the attacks were successful? How many failed and why? How could those that may have initially succeeded been prevented?

• Lab Project 4.3

Similar to Lab Project 4.2, perform a search on the Web for articles and stories about phishing attacks. Choose and read five or six articles. How many of the attacks were successful? How many failed and why? How might the successful attacks have been mitigated or successfully accomplished?